「国際レベルのセキュリティ組織へつながる道」

NSF2022

2022/3/8

自己紹介

- 武井　滋紀　です。
- JNSAのISOG-Jの方から来ました
  - ISOG-J 副代表、セキュリティオペレーション連携WG(WG6)リーダー
- NTTテクノクロス株式会社
  - セキュアシステム事業部　アソシエイトエバンジェリスト
  - 2016年度までは社名が「NTTソフトウェア株式会社」でした
  - NTTグループ セキュリティプリンシパル
  - ITU-T SG17 WP3 Q3 X.1060 Editor
  - CISSP、情報処理安全確保支援士

ISOG-J とは

- 日本セキュリティオペレーション事業者協議会
  - the Information Security Operation providers Group Japan
  - 2008年創立、2022年3月現在 58組織が加盟
  - プロのセキュリティオペレーター、事業者の集まり
  - 業界の発展のために課題を議論したり、互いに情報を出し合うことで外部へ成果を発表する団体です
  - 親団体は日本ネットワークセキュリティ協会(JNSA)
- http://isog-j.org/
  - Facebook ページ: /isogj
  - ISOG-J の読み方: いそぐじぇい

DXと言われて
セキュリティ対応組織はどうするか？

DXも変化の一つ

変化はDXだけではない

コロナ禍のテレワーク

サプライチェーン

ランサムウェア

GDPR, 改正個人情報保護法

共通する項目

セキュリティは社内システムの一つの問題ではなく、ビジネス全体の問題になった

CSIRTは設立した、でも……

変化に対応できてますか？

5年あれば状況は大幅に変わる

「セキュリティ対応組織(SOC/CSIRT)の教科書 第2.1版

2018年, 第2.1版公開

X.1060により、今、注目されている

X.1060とは

- 2021年6月29日にITU-T(国際電気通信連合の電気通信標準化部門)で国際勧告になった、サイバーリスク対応のための組織のフレームワーク

タイトル：
“Framework for the creation and operation of a cyber defence centre”

「サイバーディフェンスセンターを構築・運用するためのフレームワーク」

配布URL: https://www.itu.int/rec/T-REC-X.1060-202106-I

日本語版は？

- 2022年2月に一般社団法人　情報通信技術委員会(TTC)にて、JT-X1060が標準として決定した。
- X.1060が日本での標準として日本語で利用できます。
- 本資料の図表もこちらを引用しています。

タイトル：
「サイバーディフェンスセンターを構築・運用するためのフレームワーク」

配布URL:
https://www.ttc.or.jp/document_db/information/view_express_entity/1423

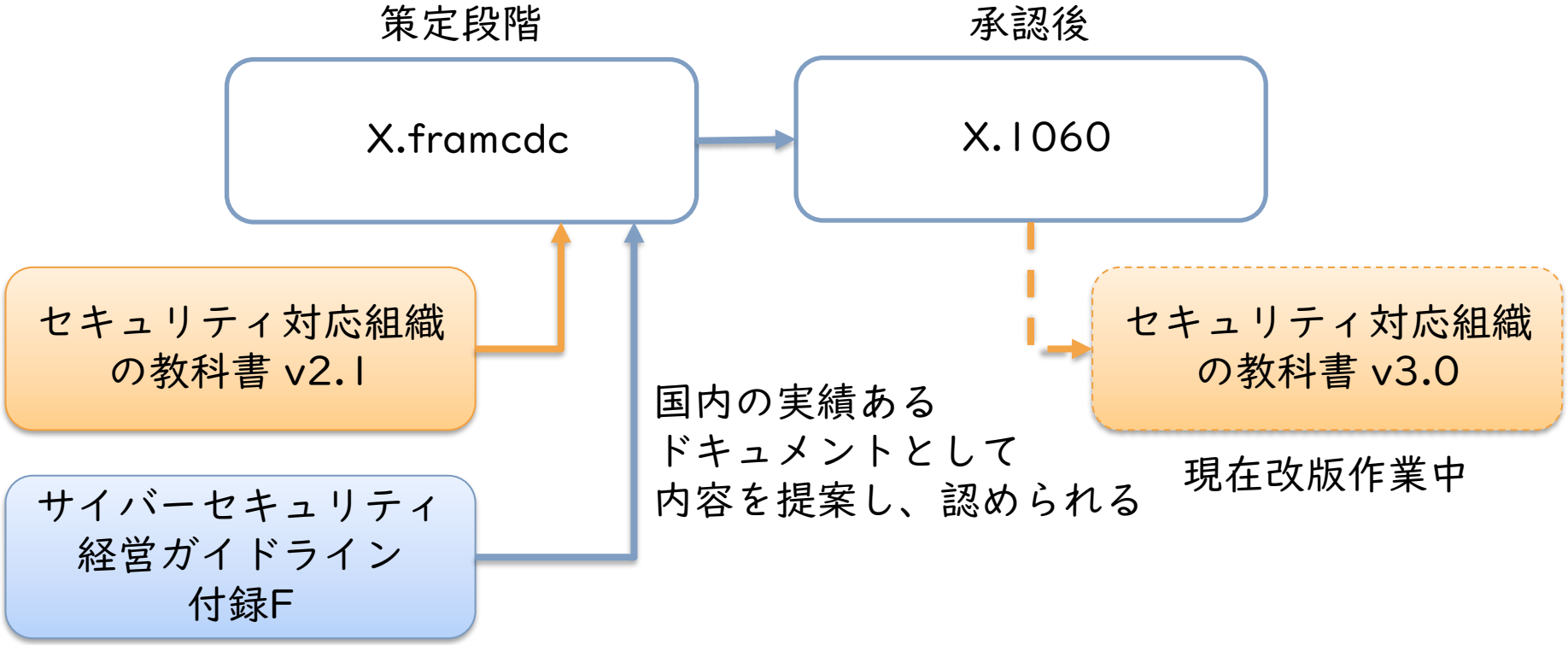
X.1060のポイント

- 新しい組織を作るわけではなく、現在のSOCやCSIRTを包含した形

- フレームワークで提示されたセキュリティサービスを実施しているなら、すでにCDCを部分的に構築していると考えられる

- 今後目指す姿として考えていただきたい

X.1060と関連ドキュメントのイメージ



X.1060における組織体制

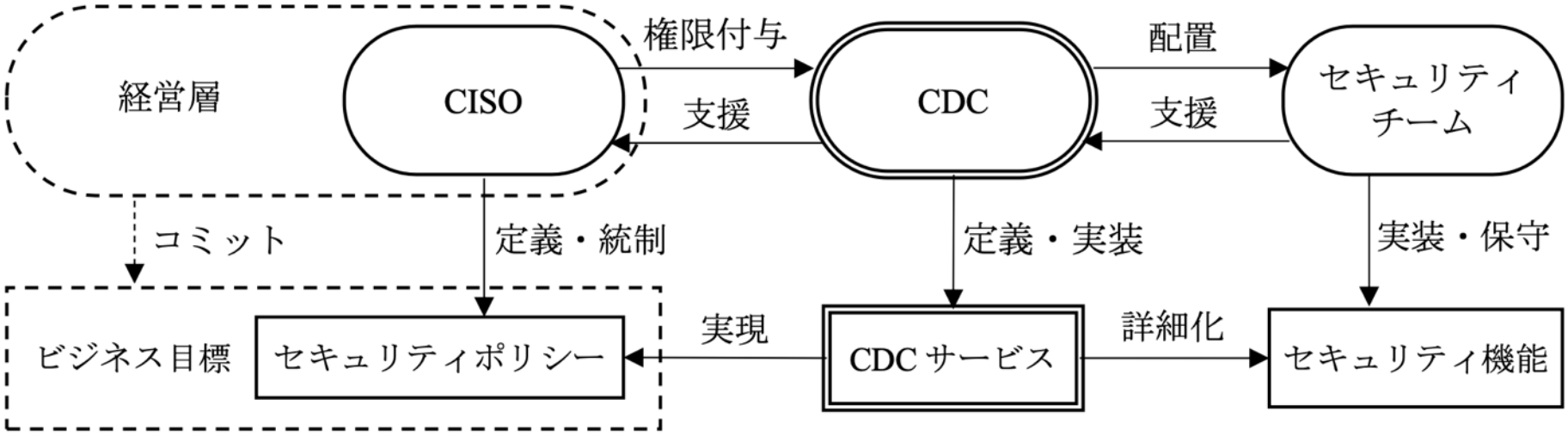


図 1　CDC の運営における関係者とその役割

図はJT-X1060より

日本のドキュメントとの比較

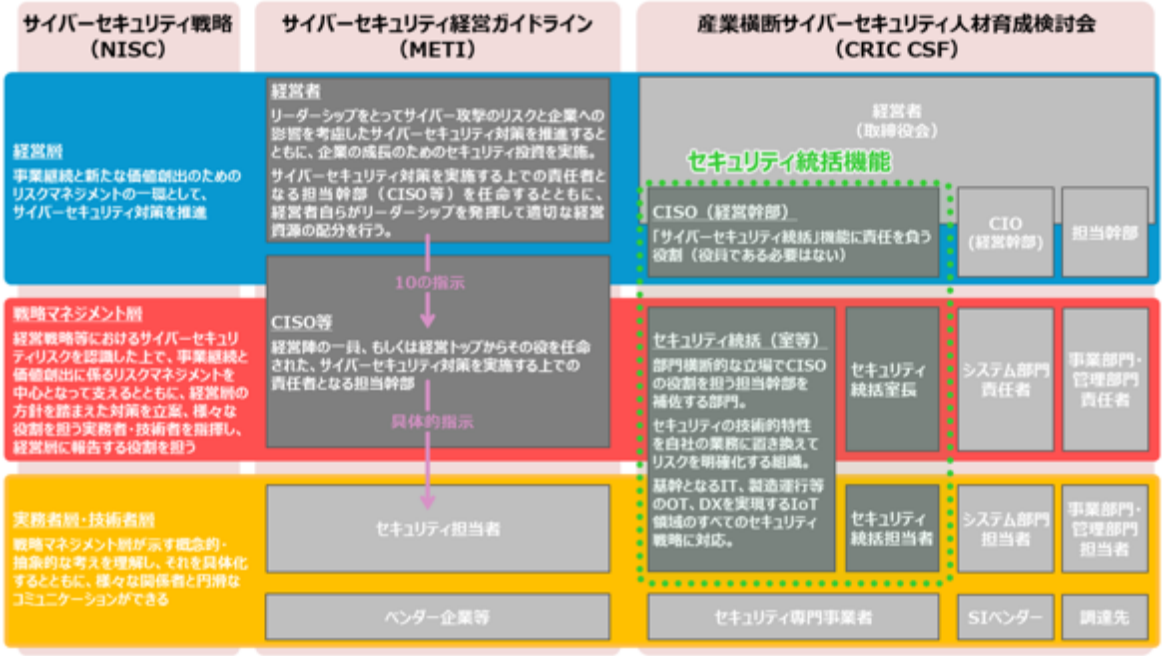


図 5　セキュリティ統括機能の位置付け（1）

経済産業省　サイバーセキュリティ経営ガイドライン
付録F サイバーセキュリティ体制構築・人材確保の手引き 第1.1版

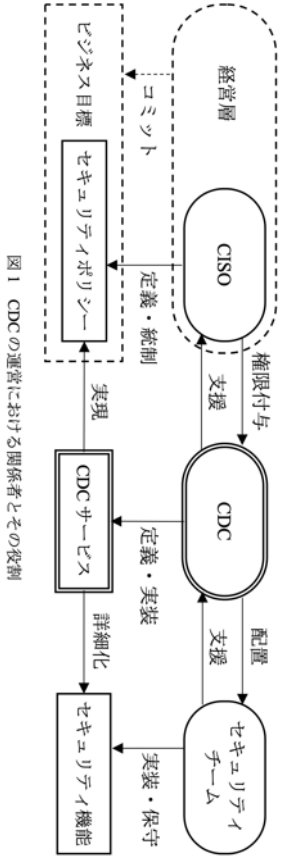


図 1　CDCの運営における関係者とその役割

各種ドキュメントとの立ち位置

フレームワーク　実践（どこで、何をするか）

X.1060

経済産業省　サイバーセキュリティ経営ガイドライン 一式

IPA サイバーセキュリティ経営ガイドライン
Ver 2.0 実践のためのプラクティス集

産業横断サイバーセキュリティ検討会
人材定義リファレンス及びスキルマッピング
ユーザ企業のためのセキュリティ統括室　構築・運用キット

日本シーサート協議会(NCA)　ドキュメント 一式
CSIRTマテリアル
CSIRT人材の定義と確保

SIM3
Security Incident Management Maturity Model

日本セキュリティオペレーション事業者協議会(ISOG-J) ドキュメント一式
セキュリティ対応組織(SOC/CSIRT)の教科書

セキュリティ対応組織アセスメント

JNSAドキュメント群

CISOハンドブック

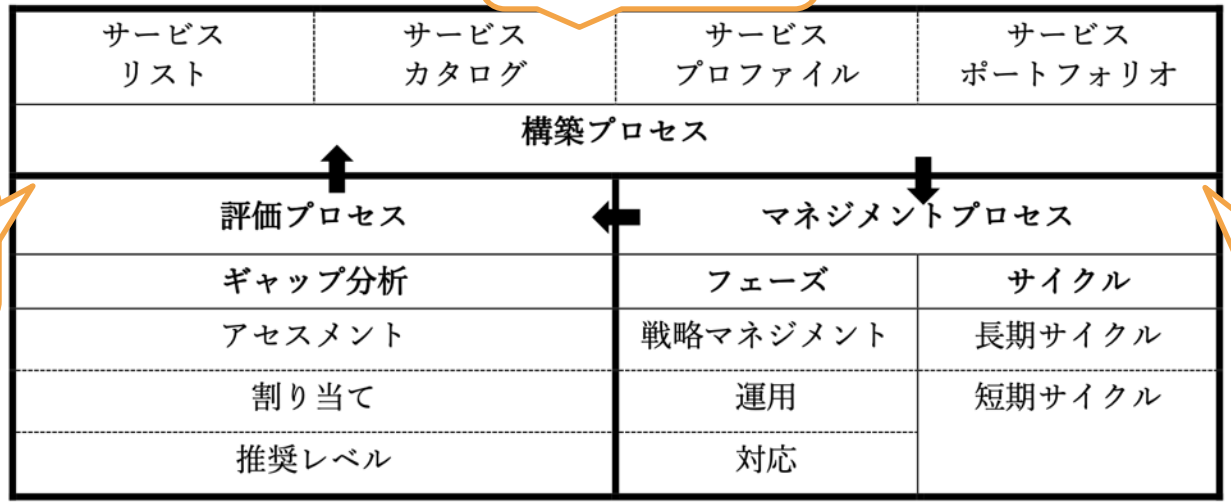
SecBok

フレームワーク概要

構築

評価

マネジメント



サービス リスト	サービス カタログ	サービス プロファイル	サービス ポートフォリオ
構築プロセス			
評価プロセス		マネジメントプロセス	
ギャップ分析		フェーズ	サイクル
アセスメント		戦略マネジメント	長期サイクル
割り当て		運用	短期サイクル
推奨レベル		対応	

図2　サイバーディフェンスセンターを構築・運用するためのフレームワーク

図はJT-X1060より

構築プロセス

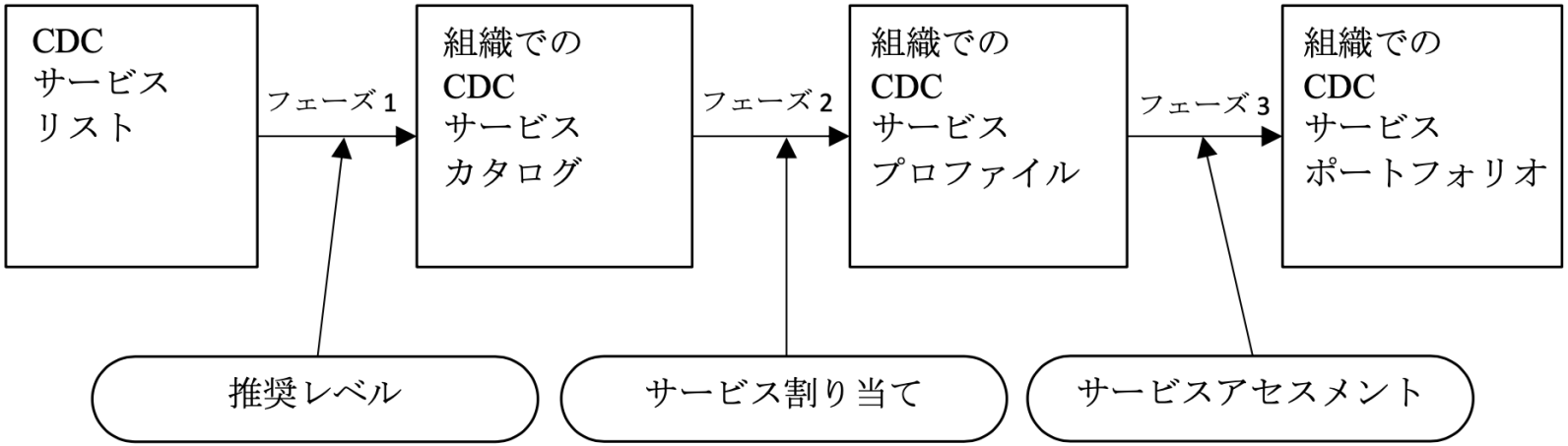


図 3　CDC サービスの立ち上げフェーズ

構築は3段階

サービスカタログ

サービスプロファイル

サービスポートフォリオ

図はJT-X1060より

構築は3つのフェーズ

サービスを選ぶ（サービスカタログを作る）

・サービスリストを参考に選び、どのサービスをどれくらいの推奨レベルで行うかを決める

どこで行うかを決める（サービスプロファイルを作る）

・それぞれのサービスは内製で実施するか、外部委託するか

今のスコアと目標のスコアを決める（サービスポートフォリオを作る）

・それぞれのサービスのスコアをセルフアセスメントで測る

構築プロセス：サービスリスト

X.1060
9つのカテゴリー
64のサービス

一覧になければ
追加しても良い

ISOG-J
9つのカテゴリー
54のサービス(※)

※ISOG-Jの教科書もX.1060に合わせて更新します。
図はJT-X1060より

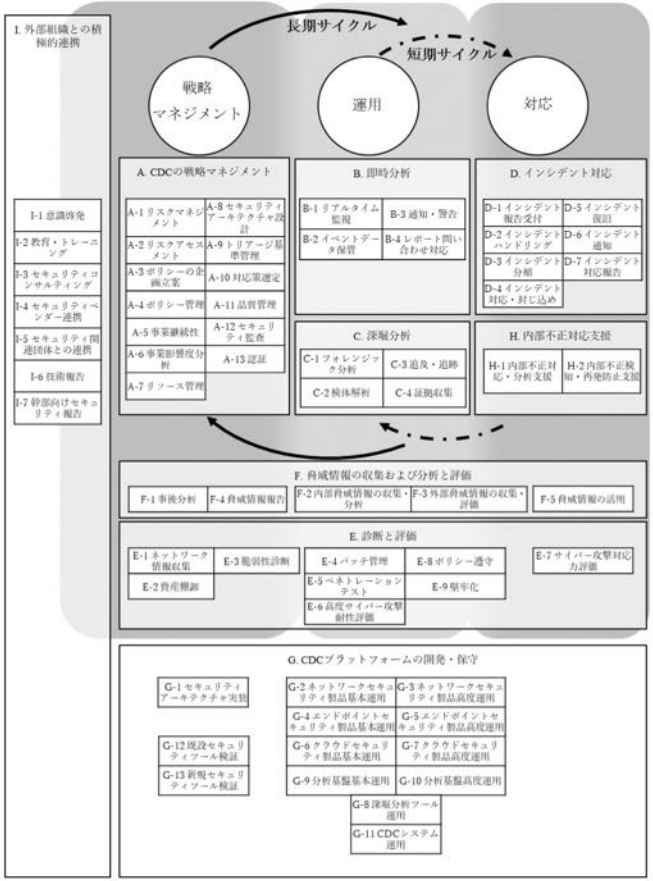


図8　CDCサービスカテゴリー

構築プロセス：サービスのアサイン

X.1060/JT-X1060

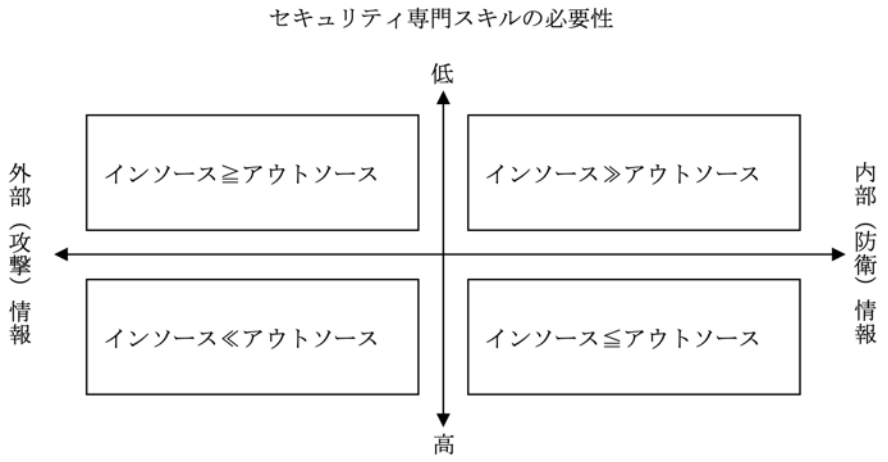


図5　調達の象限

ISOG-J

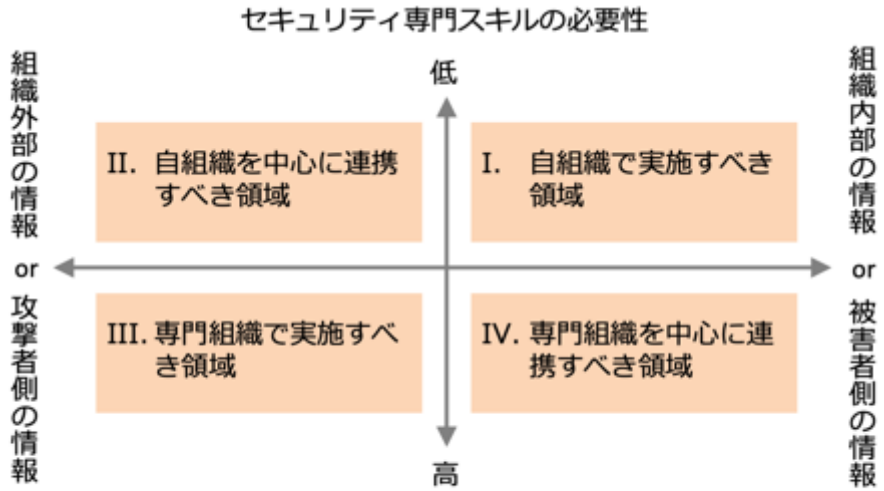


図 4　セキュリティ対応の4領域

図はJT-X1060より

構築プロセス：サービスのアセスメント

X.1060/JT-X1060

表3　CDCサービススコア

インソースの場合	
明文化された運用がCISOなど権限ある組織長に承認されている	+5点
運用が明文化されており、担当者と交代して他者が業務を実施できる	+4点
運用が明文化されておらず、担当者に代わりに他者が臨時で一部の業務を代行できる	+3点
運用が明文化されておらず、担当者のみが業務を実施できる	+2点
実施できていない	+1点
インソースとしては実施しないと決めた	適用外

アウトソースの場合	
サービス内容と得られる結果を理解でき、想定通り	+5点
サービス内容と得られる結果を理解できているが、想定未満	+4点
サービス内容、得られる結果のいずれかが理解できていない	+3点
サービス内容と得られる結果を理解できていない	+2点
結果や報告を確認できていない	+1点
アウトソースとしては実施しないと決めた	適用外

図はJT-X1060より

ISOG-J

- 自組織でその役割を実施する場合（インソース）
  - 明文化された運用はCISOなど権限ある組織長に承認されている（+5点）
  - 運用が明文化されており、担当者と交代して他者が業務を実施できる（+4点）
  - 運用が明文化されておらず、担当者に代わりに他者が臨時で一部の業務を代行できる（+3点）
  - 運用が明文化されておらず、担当者が業務を実施できる（+2点）
  - 実施できていない（+1点）
  - インソースでの実装を検討したものの、結果として実施しないと判断した（評価対象外）
- 専門組織でその役割を実施する場合（アウトソース）
  - サービス内容と得られる結果を理解でき、想定通り（+5点）
  - サービス内容と得られる結果を理解できているが、想定未満（+4点）
  - サービス内容、得られる結果のいずれかが理解できていない（+3点）
  - サービス内容と得られる結果を理解できていない（+2点）
  - 結果や報告を確認できていない（+1点）
  - アウトソースでの実装を検討したものの、結果として実施しないと判断した（評価対象外）

今後の呼び方は成熟度から変更します。

マネジメントプロセス

日々の改善を実行する

X.1060/JT-X1060

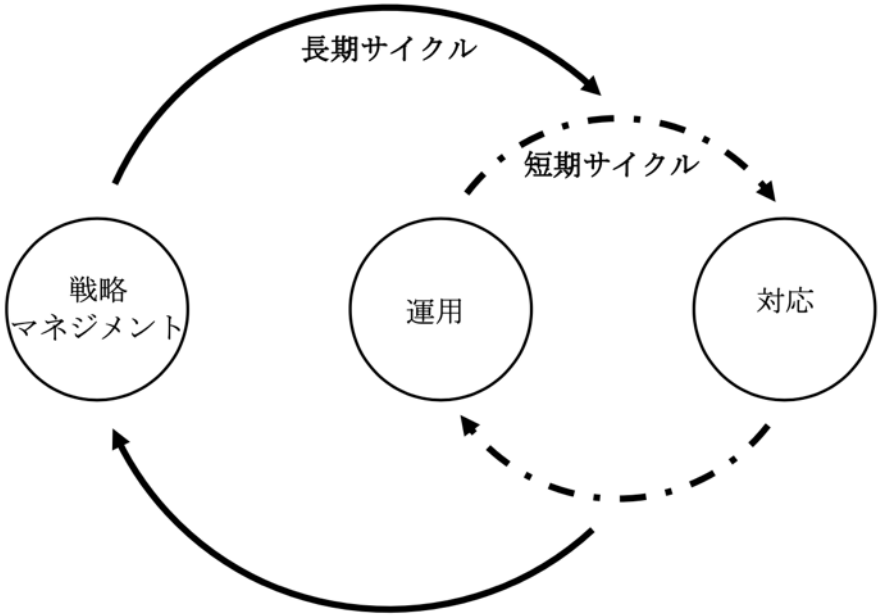


図 6　CDC マネジメントプロセス

ISOG-J

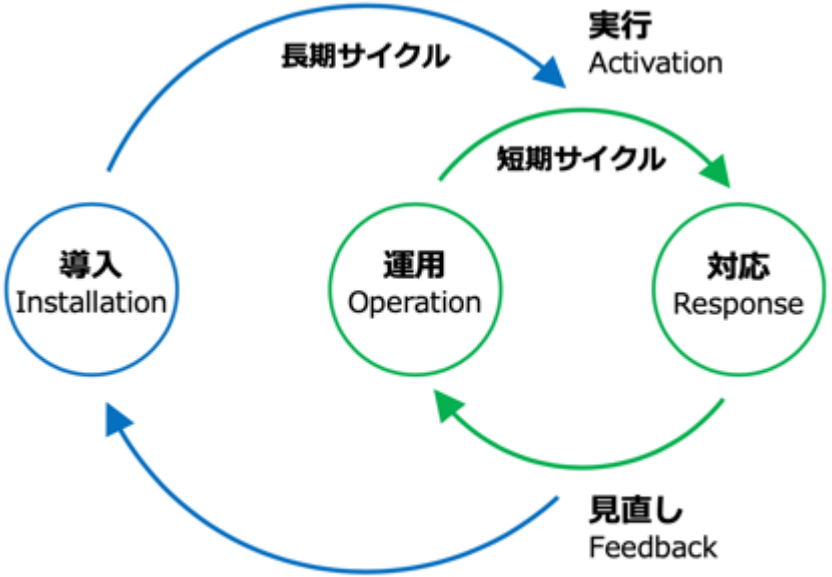
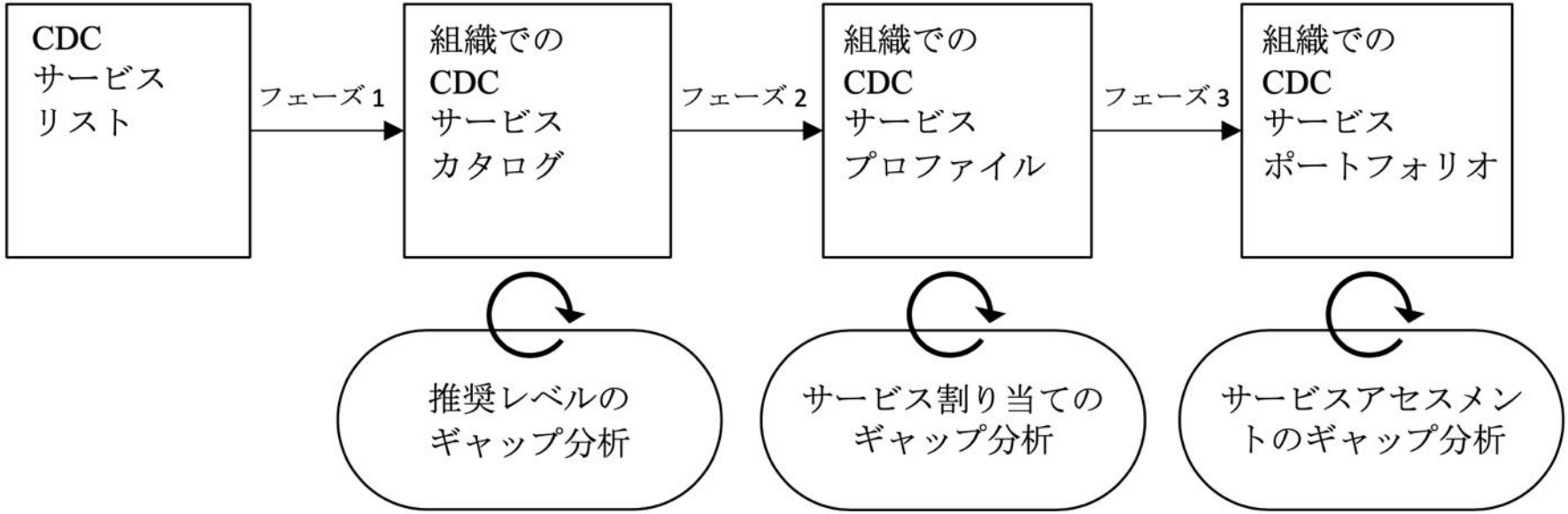


図 1　セキュリティ対応実行サイクル

図はJT-X1060より

評価プロセス



図はJT-X1060より

図 7　CDC 評価プロセス

構築で行った3つのフェーズそれぞれで見直しをする

評価は構築した3つのフェーズの振り返り

サービスを選ぶ（サービスカタログを作る）

・サービスリストを参考に選び、どのサービスをどれくらいの推奨レベルで行うかを決める

選んだものは妥当だったか？
状況の変化に対応しているか？

どこで行うかを決める（サービスプロファイルを作る）

・それぞれのサービスは内製で実施するか、外部委託するか

このままで良いか？
割り当てを変えるか？

今のスコアと目標のスコアを決める（サービスポートフォリオを作る）

・それぞれのサービスのスコアをセルフアセスメントで測る

今のスコアはどうなった？
目標は変わったか？

フレームワーク概要

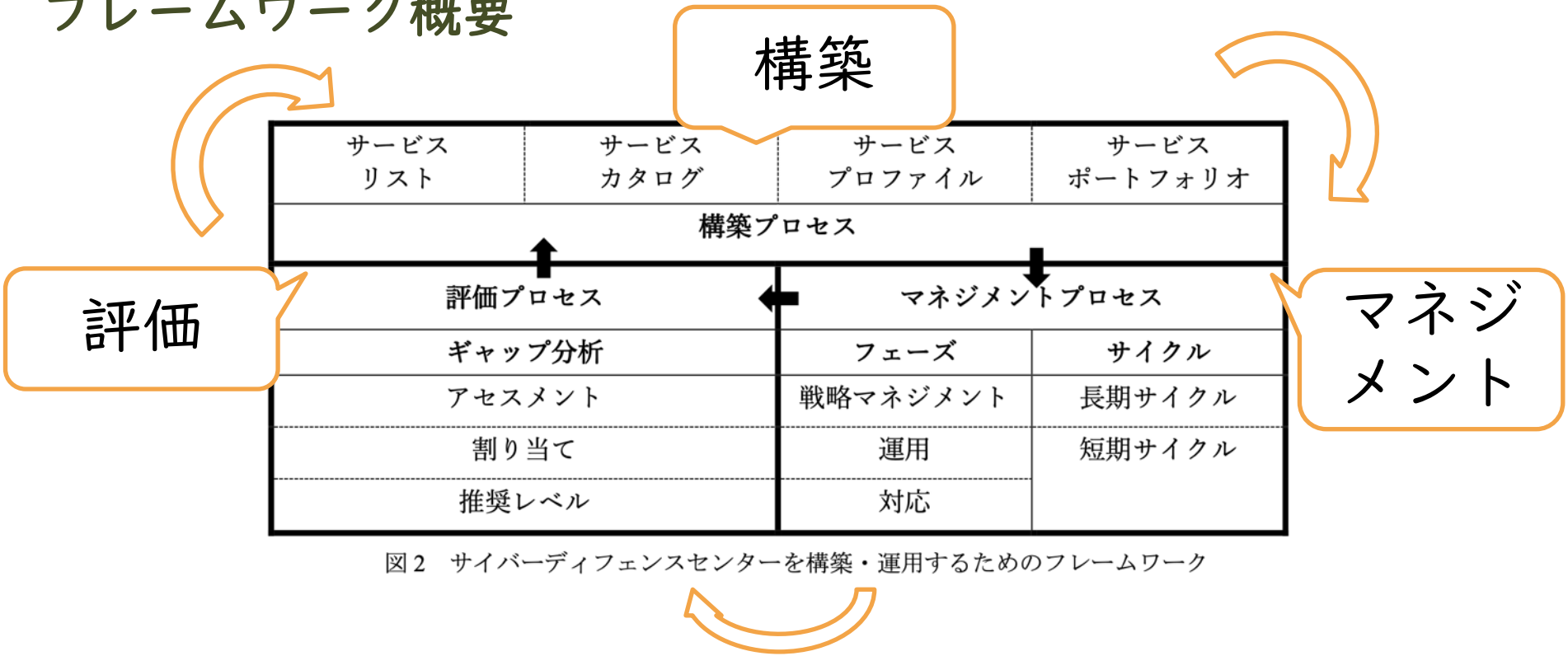


図2　サイバーディフェンスセンターを構築・運用するためのフレームワーク

図はJT-X1060より

X.1060の活用

日本のドキュメントも活用

今ある組織のこの先の姿
海外との共通理解として

まとめ

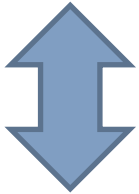
- これからも起こる変化に対応し続けるセキュリティ対応組織が必要となっている

- 継続的な改善を続けるためのフレームワークと、日本語での実用書

- これからも継続的に改善を続けて変化への対応を

X.1060を実現するための参考となるドキュメント群(ISOG-J)

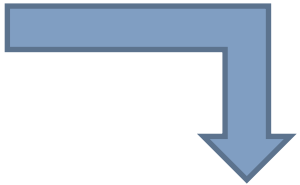
X.1060：国際標準のフレームワーク



具体的な実現方法の参考書

セキュリティ対応組織の教科書

X.1060に対応したv3.0に更新予定



情報共有の考え方

MSSの選び方

セキュリティ対応組織の強化に向けた
サイバーセキュリティ情報共有「5W1H」

マネージドセキュリティサービス選定ガイドライン

ISOG-J ホームページ
https://isog-j.org
よりダウンロード可能

セキュリティ対応組織の教科書も更新を予定しています